CLAIMS

1. A secret information management system for managing a secret information of a user, comprising:

a data division unit configured to divide the secret information into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data;

a divided data storing unit configured to store a part of the plurality of divided data into a terminal of the user as user's divided data, and a rest of the plurality of divided data into one or more of deposit servers;

a data re-division unit configured to generate a plurality of re-divided data different from the plurality of divided data obtained by the data division unit, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme; and

a re-divided data storing unit configured to store a part of the plurality of re-divided data into the terminal as newly generated user's divided data and a rest of the plurality of re-divided data into the deposit servers as newly generated divided data.

2. The secret information management system of claim 1, further comprising:

a data recovery unit configured to acquire the user's divided data, and recover the secret information from a combination of the prescribed number of the divided data among the user's divided data and the divided data stored in the deposit servers by using the secret sharing scheme, at a time of utilizing the secret information.

3. The secret information management system of claim 2, further comprising:

a utilization log memory unit configured to store a fact that the secret information is utilized as a utilization log information, at a time of utilizing the secret information.

4. The secret information management system of claim 1, further comprising:

a divided data transmission unit configured to transmit a combination of as many of the divided data stored in the deposit servers as the prescribed number minus a number of the divided data maintained by the user, to the terminal, at a time of recovering the secret information.

5. The secret information management system of claim 1, further comprising:

a transmission unit configured to transmit the part of the divided data to be stored into the terminal, to the terminal through a communication network.

6. The secret information management system of claim 1, further comprising:

a reception unit configured to receive the secret information from the terminal through a communication network.

7. The secret information management system of claim 1, wherein the data division unit and the data re-division unit use the secret sharing scheme which is a data division method for dividing the secret information into the divided data in a desired number of division according to a desired processing unit bit length, in which the divided data in the desired number of division are generated by generating a plurality of original partial data by partitioning the secret information in units of the processing unit bit

length, generating a plurality of random number partial data of the processing unit bit length from a random number in a length shorter than or equal to a bit length of the secret information, in correspondence to respective ones of the plurality of original partial data, and generating each divided partial data in the processing unit bit length that constitutes each divided data by calculating exclusive OR of the original partial data and the random number partial data, and the re-divided data in the desired number of division are generated by generating a plurality of new random number partial data of the processing unit bit length from a newly generated random number, and generating the re-divided partial data in the processing unit bit length by calculating exclusive OR of the divided partial data and the new random number partial data.

8. The secret information management system of claim 7, wherein the data re-division unit generates the re-divided data by calculating exclusive OR of the divided partial data that constitute each divided data contained in a combination of the prescribed number of the divided data.

9. The secret information management system of claim 7, wherein the data division unit and the data re-division unit use the secret sharing scheme which generates each re-divided partial data that constitutes each re-divided data by calculating exclusive OR of each divided partial data and the new random number partial data corresponding to the random number partial data used in generating each divided partial data.

10. The secret information management system of claim 9, wherein the data division unit and the data re-division unit use the secret sharing scheme in which old random number partial data are deleted from each re-divided

partial data that constitutes each re-divided data by calculating exclusive OR of each re-divided partial data and the old random number partial data used in generating each divided partial data corresponding to each re-divided partial data.

11. The secret information management system of claim 7, wherein the data division unit and the data re-division unit use the secret sharing scheme in which the desired number of division is n = 3, the divided partial data D(i,j) (i = 1 to 3, j = 1 to 2) that constitute each divided data are modified by interchanging D(1,j+1) and D(2, j+1).

12. The secret information management system of claim 7, wherein the data division unit and the data re-division unit use the secret sharing scheme in which the desired number of division is n ≥ 4, the divided partial data D(i,j) (i = 1 to n, j = 1 to n-1) that constitute each divided data are modified by setting a new value of D(1,j) to be exclusive OR of D(1,j) and D(n,j), and then rotating D(1,j), D(2,j), ····· D((n-1),j).

13. The secret information management system of claim 12, wherein the data division unit and the data re-division unit use the secret sharing scheme in which D(1,j), D(2,j), ····· D((n-1),j) are rotated for (i-1) times.

14. The secret information management system of claim 7, wherein the data re-division unit generates the plurality of re-divided data from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers and the user's divided data stored in the terminal, upon receiving the user's divided data from the terminal, and

the re-divided data storing unit stores a part of the plurality of re-divided data into another terminal of another user as another user's divided data and a rest of the plurality of re-divided data into the deposit servers as new divided data, at a time of transferring an access right for the secret information from the user to the another user.

15. A secret information management method for managing a secret information of a user, comprising the steps of:

dividing the secret information into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data;

storing a part of the plurality of divided data into a terminal of the user as user's divided data, and a rest of the plurality of divided data into one or more of deposit servers;

generating a plurality of re-divided data different from the plurality of divided data obtained by the dividing step, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme; and

storing a part of the plurality of re-divided data into the terminal as newly generated user's divided data and a rest of the plurality of re-divided data into the deposit servers as newly generated divided data.

16. A computer program product for causing a computer to function as a secret information management system for managing a secret information of a user, the computer program product comprising:

a first computer program code for causing the computer to divide the secret information into a plurality of divided data by using a secret sharing scheme, such that

the secret information can be recovered from a prescribed number of the divided data;

a second computer program code for causing the computer to store a part of the plurality of divided data into a terminal of the user as user's divided data, and a rest of the plurality of divided data into one or more of deposit servers;

a third computer program code for causing the computer to generate a plurality of re-divided data different from the plurality of divided data obtained by the first computer program code, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme; and

a fourth computer program code for causing the computer to store a part of the plurality of re-divided data into the terminal as newly generated user's divided data and a rest of the plurality of re-divided data into the deposit servers as newly generated divided data.